



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,629	08/16/2001	Steven Dale Goodman	RPS9 2001 0046	2708

45211 7590 09/20/2005

KELLY K. KORDZIK
WINSTEAD SECHREST & MINICK PC
PO BOX 50784
DALLAS, TX 75201

EXAMINER

CHAI, LONGBIT

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 09/20/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/931,629

Applicant(s)

GOODMAN ET AL.

Examiner

Longbit Chai

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 15 July 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☐ Claim(s) _____ is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-4 and 6-10 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 16 August 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1 – 10 have been presented for examination. Claim 5 has been canceled; claim 4 has been amended in an amendment filed 7/15/2005. Therefore, presently pending claims are 1 – 4 and 6 – 10.

Response to Arguments

2. Applicant's arguments filed on 7/15/2005 with respect to the subject matter of the instant claims have been fully considered but are not persuasive.

3. Applicant remarks, on page 6, the combination of Alexander and Grawrock does not teach a TPM performing a signature verification of an update to a program because Grawrock teaches the verification of the BIOS occurs after it has already been loaded onto the system (also shown in the "1.132 declaration" filed on 2/17/2005). Examiner notes this subject matter has been fully considered but is not persuasive. First of all, the Alexander reference is relied upon validating the BIOS data prior to loading the new BIOS update image (Alexander: Column 5 Line 41 – 45: allow the loading only if a valid RBU image exists). Besides, the reliance of the signature verification performed at TPM on the BIOS image is laid upon the Grawrock reference (Grawrock: Column 4 Line 1 – 18) and therefore applicant's arguments are respectfully traversed.

Double Patenting

4. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and, *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

5. Claims 1, 4 and 8 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 18 (and claim 3) of copending Application No. 09931550.

This is a provisional obviousness-type double patenting rejection. The subject matter claimed in the instant application is fully disclosed in the co-pending Application

Art Unit: 2131

since both applications are claiming common subject matter except the features of using SMI (System Management Interrupt) specifically claimed by co-pending Application. Furthermore, there is no apparent reason why applicant was prevented from presenting claims corresponding to those during prosecution of the co-pending Application.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A person shall be entitled to a patent unless –

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1 – 4 and 6 –10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alexander (Patent Number: 6188602), in view of Grawrock (Patent Number: 6678833).

With regards to claim 1, Alexander teaches a method for updating a program in a data processing system comprising the steps of:

modifying the program with the update to the program in response to the unlocking of the memory unit storing the program (Alexander: Column 5 Line 46 – 52, Column 5 Line 41 – 45 and Column 5 Line 60 – 61).

Alexander fails to teach the use of a trusted platform module ("TPM") to perform a signature verification of an update to the program.

Grawrock teaches:

requesting a trusted platform module ("TPM") to perform a signature verification of an update to the program; and the TPM performing the signature verification of the update to the program (Grawrock: Column 4 Line 1 – 18; Alexander: Column 5 Line 41 – 45: Examiner notes First of all, the Alexander reference is relied upon validating the BIOS data prior to loading the new BIOS update image (Alexander: Column 5 Line 41 – 45: allow the loading only if a valid RBU image exists). Besides, the reliance of the signature verification performed at TPM on the BIOS image is laid upon the Grawrock reference (Grawrock: Column 4 Line 1 – 18));

if the signature verification of the update to the program is successful, unlocking a memory unit storing the program (Alexander, Column 5 Line 41 – 45 and Column 5 Line 58 – 62; Grawrock, Column 4 Line 1 – 18).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Grawrock's TPM within the system of Alexander's memory device because it offers the advantages of allowing the TPM to accurately report the identity of the boot block without reliance on any intervening devices (Grawrock: Column 2 Line 1 – 6).

With regards to claim 2, 6 and 9, Alexander teaches locking the memory unit after the modifying step (Alexander: Column 5 Line 62 – 64).

With regards to claim 3, Alexander teaches the locking step is performed by the TPM (Alexander: Column 5 Line 62 – 64, Grawrock: Column 4 Line 1 – 9).

With regards to claim 4, Alexander teaches a computer program product adaptable for storage on a computer readable medium and operable for updating a BIOS stored in a flash memory in a data processing system, comprising:

a BIOS update application program receiving an updated BIOS image
(Alexander: Column 5 Line 1 – 13);

the BIOS update application modifies the BIOS with the updated BIOS image
(Alexander: Column 5 Line 41 – 45);

Alexander fails to teach the use of TPM to perform a signature verification of an update to the program.

Grawrock teaches:

the BIOS update application requesting a TPM to perform a signature verification of the updated BIOS image (Grawrock: Column 4 Line 1 – 18; Alexander: Column 5 Line 46 – 52);

a TPM program receiving the request from the BIOS update application to perform the signature verification of the updated BIOS image (Grawrock: Column 4 Line 1 – 18; Alexander: Column 5 Line 30 – 67); and

the TPM program performing the signature verification of the updated BIOS image and posting a result of the signature verification of the updated BIOS image to

the BIOS update application (Grawrock: Column 4 Line 1 – 9; Alexander: Column 5 Line 30 – 67);

if the result of the signature verification of the updated BIOS image determines that the updated BIOS image is authentic, then the TPM program unlocks the flash memory (Alexander: Column 5 Line 58 – 62, Grawrock: Column 4 Line 1 – 9; Alexander: Column 5 Line 30 – 67).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Grawrock's TPM within the system of Alexander's memory device because it offers the advantages of allowing the TPM to accurately report the identity of the boot block without reliance on any intervening devices (Grawrock: Column 2 Line 1 – 6).

With regards to claim 7 and 10, Alexander teaches if the result of the signature verification of the updated BIOS image determines that the updated BIOS image is not authentic, then an error message is output (Grawrock: Column 5 Line 34 – 38; Alexander: Column 5 Line 36 – 40).

With regards to claim 8, Alexander teaches a data processing system having circuitry for updating a BIOS stored in a flash memory in the data processing system, comprising:

circuitry for modifying the BIOS with the updated BIOS image (Alexander: Column 5 Line 41 – 45).

Alexander fails to teach the use of TPM to perform a signature verification of an update to the program.

Grawrock teaches:

input circuitry for receiving an updated BIOS image (Grawrock: Figure 3 & Column 3 Line 50 – 56; Alexander: Column 5 Line 30 – 67);

circuitry for requesting a TPM to perform a signature verification of the updated BIOS image (Grawrock: Figure 3 & Column 4 Line 10 – 18; Alexander: Column 5 Line 30 – 67);

the TPM performing the signature verification of the updated BIOS image (Grawrock: Figure 3 & Column 3 Line 1 – 19; Alexander: Column 5 Line 30 – 67);

the TPM unlocking the flash memory if the signature verification of the updated BIOS image determines that the updated BIOS image is authentic (Alexander: Column 5 Line 58 – 62; Grawrock: Column 4 Line 1 – 9).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Grawrock's TPM within the system of Alexander's memory device because it offers the advantages of allowing the TPM to accurately report the identity of the boot block without reliance on any intervening devices (Grawrock: Column 2 Line 1 – 6).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131


LBC


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100